WHAT IS CLAIMED IS:

Sub A1

1. In a computer system, a method comprising:

receiving information indicative of a possible change to a protected file; and

determining whether the change is valid by verifying the file, and if not valid, preventing the change.

2. The method of claim 1 wherein receiving information indicative of a possible change includes receiving notification indicative of a change to a protected file.

3. The method of claim 1 wherein receiving information indicative of a possible change includes receiving notification of a change to a file, and accessing information to determine whether the file is protected.

4. The method of claim 1 wherein preventing the change includes overwriting a changed copy of the file with a valid copy of the protected file.

5. The method of claim 1 wherein preventing the change includes discarding change data.

6. The method of claim 1 wherein determining whether the change is valid by verifying the file includes obtaining cryptographic hash information of the changed file and comparing the cryptographic hash information against cryptographic hash information associated with the protected file.

A1

7. The method of claim 6 wherein comparing the cryptographic hash information includes accessing a catalog of information for protected files.

8. The method of claim 1 wherein determining whether the change is valid includes determining whether the file includes a signature.

9. The method of claim 1 further comprising, monitoring files in a file system.

10. The method of claim 1 wherein preventing the change includes copying a valid copy of the protected file to a former location of the protected file.

11. The method of claim 10 wherein copying a valid copy of the protected file includes finding a file having the same identity as the protected file.

12. The method of claim 11 wherein finding the file having the same identity as the protected file includes accessing a cache.

13. The method of claim 12 further comprising verifying the file having the same identity.

A1

14. The method of claim 11 wherein finding the file having the same identity as the protected file includes accessing a network.

15. The method of claim 14 further comprising verifying the file having the same identity.

16. The method of claim 15 wherein finding the file having the same identity as the protected file includes accessing a recorded medium.

17. The method of claim 16 further comprising verifying the file having the same identity.

18. The method of claim 1 wherein preventing the change includes discarding change data and returning a success to a component.

19. The method of claim 1 further comprising receiving information indicating that a protected file is about to be changed, preserving a copy of the protected file, and wherein preventing the change includes overwriting a changed copy of the file with a copy of the protected file that was preserved.

A1

20. A computer-readable medium having computer-executable instructions, comprising:

(1) selecting a plurality of files as protected files;

(2) receiving information indicative of a possible change to a protected file;

(3) determining whether the file is an exception case, and

(a) if an exception case, allowing the change, or

(b) if not an exception case, determining whether the change is valid by verifying the file, and

(i) if valid, allowing the change; and

(ii) if not valid, preventing the change.

21. The computer-readable medium of claim 20 wherein receiving information indicative of a possible change includes receiving notification indicative of a change to a protected file.

22. The computer-readable medium of claim 20 wherein receiving information indicative of a possible change includes receiving notification of a change to a file, and accessing information to determine whether the file is protected.

23. The computer-readable medium of claim 20 wherein preventing the change includes overwriting a changed copy of the file with a valid copy of the protected file.

24. The computer-readable medium of claim 20 wherein preventing the change includes discarding change data.

25. The computer-readable medium of claim 20 further comprising returning information indicative of a success.

26. The computer-readable medium of claim 20 wherein allowing the change includes writing data saved via a copy-on-write process to the file.

27. The computer-readable medium of claim 20 wherein determining whether the file is an exception case includes checking a security descriptor of the file.

28. The computer-readable medium of claim 20 further comprising providing a prompt before allowing a change.

29. The computer-readable medium of claim 20 wherein determining whether the change is valid includes obtaining cryptographic hash information of the changed file, and comparing the cryptographic hash information against cryptographic hash information associated with the protected file.

30. The computer-readable medium of claim 20 wherein determining whether the change is valid includes determining whether the file includes a signature.

31. A computer system, comprising,

a protected file,

a detection mechanism configured to determine when the protected file may be changed,

a verification mechanism; and

a file protection service, the file protection service configured to receive a determination from the detection mechanism that the protected file may be changed, and further configured to communicate with the verification mechanism to verify whether the change is valid, and to prevent the change when the change is not valid.

32. The computer system of claim 31 wherein the detection mechanism includes a mechanism for monitoring at least one directory for changes to at least one file therein.

33. The computer system of claim 31 wherein the detection mechanism provides a notification to the file protection service as the determination mechanism that the protected file may be changed.

34. The computer system of claim 31 wherein the file protection service accesses a data structure to determine whether the notification received from the detection mechanism corresponds to a protected file.

35. The computer system of claim 31 wherein the file protection service is incorporated into a file system.

36. The computer system of claim 31 wherein the file protection service prevents the change by discarding changed data.

37. The computer system of claim 36 wherein the file protection service returns information indicative of a success.

38. The computer system of claim 31 wherein the verification mechanism verifies whether the change to a file is valid by comparing a cryptographic hash of the file contents against a cryptographic hash associated with a valid file.

39. The computer system of claim 38 wherein the cryptographic hash associated with a valid file is maintained in a data structure including a cryptographic hash of the contents of at least one other protected file.

40. The computer system of claim 31 wherein the file protection service prevents the change by copying valid data over changed data.

41. The computer system of claim 40 wherein the file protection service locates valid data in a system cache.

42. The computer system of claim 40 wherein the file protection service locates valid data at a network share.

43. The computer system of claim 40 wherein the file protection service locates valid data in a recorded medium.

44. The computer system of claim 40 wherein the file protection service locates valid data in a preserved location.

45. The computer system of claim 31 further comprising a scanning mechanism for causing a plurality of files to trigger the detection mechanism.